III. Amendments to the Specification

Please amend the specification by deleting the noted original paragraphs and replacing them with the following versions of the paragraphs.

Page 1, lines 4-10:

The following co-pending applications are all assigned to the assignee of the invention and are incorporated herein by reference:

1. U.S. Serial No. 09/738,240, ~~_____~~, entitled "Configurable PKI Architecture" filed on 12/15/2000; ~~_____ in the names of _____;~~ and

2. U.S. Serial No. 09/738,239, ~~_____~~, entitled "Dynamic Modular PKI Architecture" filed on 12/15/2000. ~~_____ in the names of _____;~~

Page 8, lines 24-30:

Additional computing components connected to the network 102 ~~10~~ may include a personal digital assistant 114 and a remote network appliance 116. Additionally, an individual user may carry a so-called "smart card" 118. The smart card may contain sufficient data and/or processing capabilities to allow connection to and communication with other components of the distributed data processing system 100.

Page 12, lines 1-10:

Typically, after the CA has received a request for a new digital certificate, which contains the requesting entity's public key, the CA puts ~~signs~~ the requesting entity's public key into a certificate and signs the certificate with the CA's private key. ~~with the CA's private key and places the signed public key within the digital certificate.~~ Anyone who receives the digital certificate during a transaction or communication can then use the public key of the CA to verify the signed public key within the certificate. The intention is that an entity's certificate verifies that the entity owns a particular public key.

Page 13, lines 11-18:

Other aspects of certificate processing are also standardized. The Certificate Request Message Format (RFC 2511) specifies a format recommended for use whenever a relying party is requesting a certificate from a CA. Certificate Management Protocols have also been promulgated for transferring certificates. More information about the X.509 public key infrastructure (PKIX) can be obtained from the Internet Engineering Task Force (IETF) at "www.ietf.org". ~~www.ietf.org.~~

Page 14, lines 1-18:

Figure 2 is a block diagram depicting a typical manner in which an individual obtains a digital certificate. User 202, operating on some type of client computer, has previously obtained or generated a public/private key pair, e.g., user public key 204 and user private key 206. User 202 generates a request for certificate 208 containing user public key 204 and sends the request to certifying authority 210, which is in possession of CA public key 212 and CA private key 214. Certifying authority 210 verifies the identity of user 202 in some manner and generates X.509 digital certificate 216 containing ~~signed~~ user public key 218, ~~216 that was~~ and the certificate is signed with CA private key 214. User 202 receives newly generated digital certificate 216, and user 202 may then publish digital certificate 216 as necessary to engage in trusted transactions or trusted communications. An entity that receives digital certificate 216 may verify the signature of the CA by using CA public key 212, which is published and available to the verifying entity.

Page 16, lines 1-9:

Furthermore, a specific PKI solution may be built from the ground up. For example, one application may need a simple CA that is able to issue certificates and manage the life cycle of the ~~these~~ certificates including revocation of certificates and generating certificate revocation lists. Another application used by the same entity may also issue certificates in bulk and have support for multiple applications and/or identification procedures. As such, a readily adaptable and lightweight system is described herein for the implementation of any such PKI technology.

Page 17, lines 23-27:

Likewise, if the request from the network 310 ~~300~~ is in the form of a Public Key Cryptography Standard #10 (PKCS10) format, a PKCS10 server bean 322 ~~312~~ fields such a request and formats this type of request for transmittal to the remainder of the system 300.

Page 18, lines 20-28:

After clearing the auditor bean 360, the request may then be sent to a Lightweight Directory Access Protocol (LDAP) publisher bean 370. This LDAP publisher bean 370 publishes certificates or certificate revocation lists, which may be obtained in ~~any specific parameters associated with such a request to an LDAP directory structure 373. Again, this may take place as the request winds its way through the PKI request system 300 an initial time. Or the publishing of the request in the LDAP directory 373 may take place in~~ the return path of the requests ~~request~~ after reaching the terminus bean.

Page 19, lines 18-22:

Returning now to our exemplary system, the request now reaches an X.509 generator bean 380. ~~330.~~ This bean 380 ~~330~~ generates the digital certificate based upon the X.509 specification that defines digital certificates containing signed user public keys.

Page 24, lines 5-8:

As a final step in this example, the request is selectively directed to a particular path or bean from a selection of beans. This takes place in an IfThenElse bean 446 or 448.